AO 106 (Rev. 01/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT FILED NOV 16 2017 MARY C. LOEWENGUTH, CLERK WESTERN DISTRICT OF NY

UNITED STATES DISTRICT COURT

for the

Western District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address.)

Premises located at 102 Mitchell Lane, Hamlin, New York 14464 and the Person of David Daniel, Jr.

Case No. 17-MJ- 622

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of New York *(identify the person or describe property to be searched and give its location):* **The premises located at 102 Mitchell Lane, Hamlin, New York 14464 and the Person of David Daniel, Jr. as described in Attachment A.**

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*: **See Attachment B for the Items to be Seized, all of which are evidence and instrumentalities of violations of Title 18 United States Code, Sections 2252A(a)(5)(B) and 2252A(a)(2)(A) and (B), and all of which are more fully described in the application and affidavit filed in support of this warrant, the allegations of which are adopted and incorporated by reference as if fully set forth herein.**

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

__X__ evidence of a crime;
__X__ contraband, fruits of crime, or other items illegally possessed;
__X__ property designed for use, intended for use, or used in committing a crime;
_____ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of **18** U.S.C. §§ **2252A(a)(5)(B) and 2252A(a)(2)(A) and (B)**, and the application is based on these facts which are continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Justin Burnham, Special Agent, H.S.I.
Printed name and title

Sworn to before me and signed in my presence.

Date: 11/16/17

Judge's signature

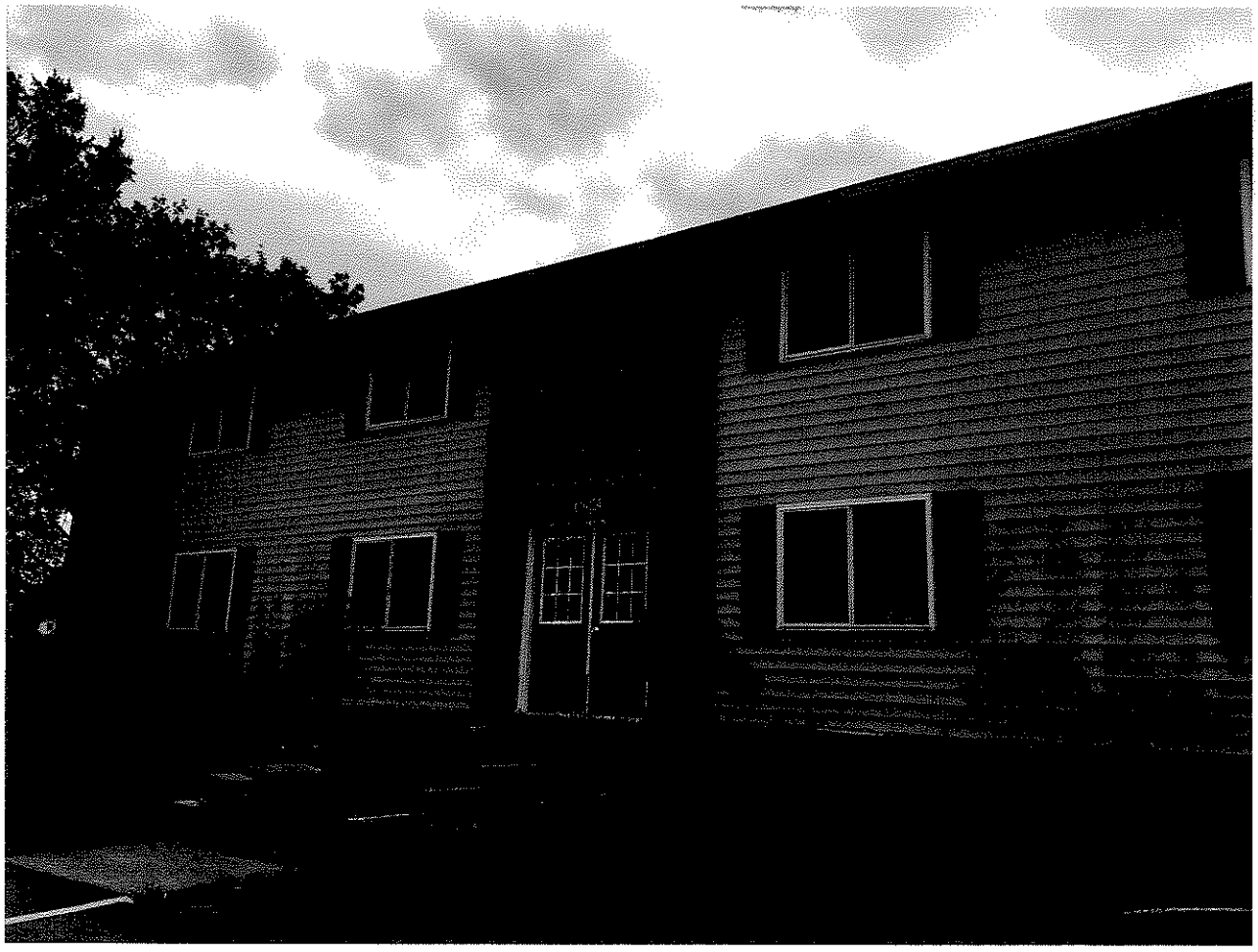
City and state: Rochester, New York

Jonathan W. Feldman, United States Magistrate Judge
Printed name and title

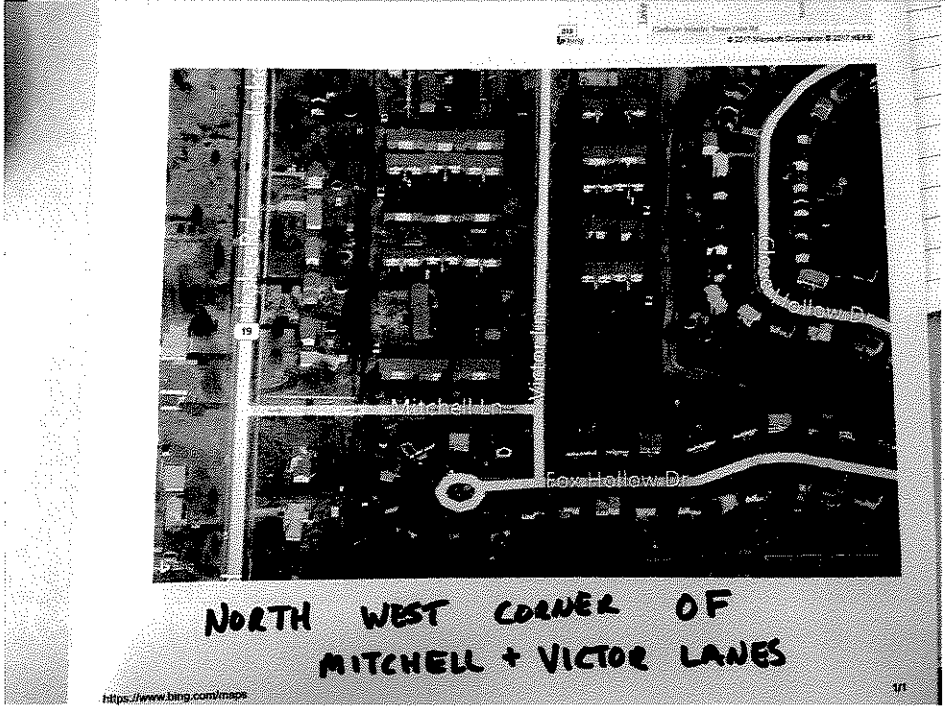
ATTACHMENT A

DESCRIPTION OF THE SUBJECT PREMISES

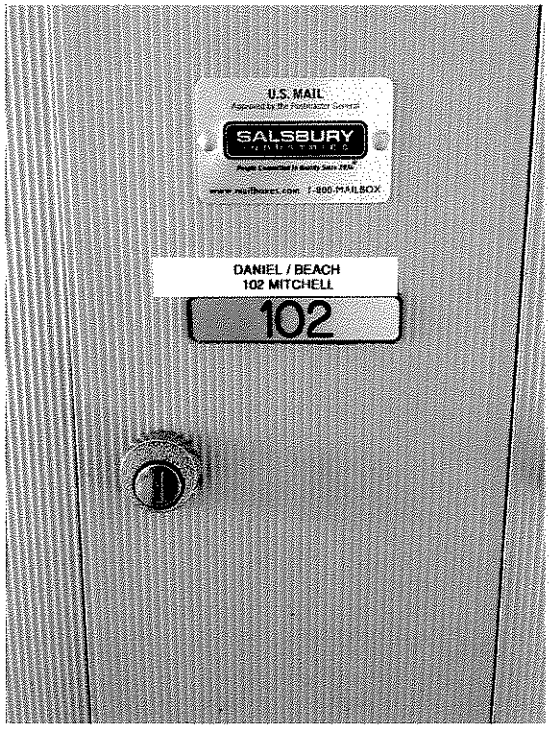
The SUBJECT PREMISES, 102 Mitchell Lane, Hamlin, New York, 14464, is a single apartment, designated as 102, on the lower level of the two-story apartment complex depicted below. The apartment is located at the intersection of Mitchell Lane and Victor Lane as depicted in the attached maps. The front door to apartment 102 is white in color and is designated with the number "102" as depicted in the photographs below.




102 Mitchell Ln, Hamlin, NY 14464
MITCHELL LANE
VICTOR LANE


Victor Ln
Mitchell Ln
Fox Hollow Dr
Glen Hollow Dr
NORTH WEST CORNER OF
MITCHELL + VICTOR LANES
https://www.bing.com/maps


102


U.S. MAIL
SALSBURY
DANIEL / BEACH
102 MITCHELL
102

DESCRIPTION OF THE SUBJECT PERSON

Name:	David W. Daniel Jr.
Date of Birth:	September 1, 1980
Height:	6'02"
Last Known Address:	102 Mitchell Lane, Hamlin New York, 14464

ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations 2252A(a)(2)(A) (possession of child pornography) and 2252A(a)(5)(B) (receipt and distribution of child pornography):

1. Computers or storage media used as a means to commit the violations described above, including but not limited to cellular phones.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. evidence of the lack of such malicious software;

    d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

    e. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the SUBJECT PREMISES, including utility and telephone bills, mail envelopes, or addressed correspondence;

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of "Application A";

e. Records and information showing access to and/or use of "Application A"; and

f. Records and information relating or pertaining to the identity of the person or persons using or associated with the username "mrngstr."

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

STATE OF NEW YORK)
COUNTY OF MONROE) SS:
CITY OF ROCHESTER)

JUSTIN BURNHAM, being duly sworn, deposes and states:

1. I am a Special Agent with Homeland Security Investigations (HSI) and have been so employed since October 2008. I am currently assigned to the Buffalo Field Office and am a member of the Child Exploitation Unit (CEU). As a member of the CEU, I investigate crimes involving the sexual exploitation of children, including the possession, receipt and distribution of child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(a)(2)(A) and (B). I have received specialized training in the area of child pornography and child exploitation, and have observed numerous examples of child pornography as defined in 18 U.S.C. § 2256.

2. This affidavit is submitted pursuant to Rule 41 of the Federal Rules of Criminal Procedure in support of an application for a search warrant for the person of DAVID DANIEL, JR. (hereinafter the "SUBJECT PERSON") as well as the premises located at 102 Mitchell Lane, Hamlin, New York 14464 (hereinafter the "SUBJECT PREMISES"), including the content of electronic storage devices located therein. The SUBJECT PREMISES are more particularly described in **Attachment A** of this Affidavit. The items to be seized include contraband, evidence, fruits and instrumentalities involving the possession, receipt and distribution of child pornography in violation of 18 U.S.C.

§§ 2252A(a)(5)(B) and 2252A(a)(2)(A) and (B), more specifically described in **Attachment B** of this Affidavit.

3. The statements in this affidavit are based in part on information provided by HSI agents in Ottawa, Canada, and on my investigation of this matter. Since this affidavit is submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts sufficient to establish probable cause that contraband, evidence, fruits and instrumentalities involving the possession, receipt and distribution of child pornography are presently located at the SUBJECT PREMISES or on the SUBJECT PERSON.

STATUTORY AUTHORITY

4. As stated above, this investigation concerns alleged violations of 18 U.S.C. §§ 2252A(a)(2)(A) and (B) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography).

5. 18 U.S.C. §§ 2252A(a)(2)(A) and (B) prohibit a person from knowingly receiving or distributing any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

6. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, any material that contains an image of child

pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

PROBABLE CAUSE

7. Canadian law enforcement officers have reported to HSI that on March 22, 2016, an officer with the Saskatchewan Police Service (SPS) in Saskatchewan, Canada, arrested an individual (hereinafter "John Doe") for parole violations.[1] Pursuant to the arrest, SPS seized John Doe's iPhone. John Doe told SPS that he had been using an online mobile chat application to download and distribute child pornography images and videos to a network of other users of the mobile chat application. He provided SPS his username and login information for the application and gave SPS consent to take over and use his account to conduct investigations and gather evidence with respect to other users. This chat application is hereinafter referred to as "Application A."[2] HSI was not involved with the user's arrest.

[1] John Doe's true name is known to law enforcement. This investigation remains active and disclosure of Doe's true name would potentially alert investigative suspects to the fact that law enforcement action is being taken, thereby provoking suspects to notify other users of law enforcement action, flee, and/or destroy evidence.

[2] The actual name of "Application A" is known to law enforcement. This chat application remains active and disclosure of the name of the application would potentially alert its users to the fact that law enforcement action is being taken against users of the application, thereby provoking users to notify other users of law enforcement action, flee, and/or destroy evidence. Accordingly, to protect the confidentiality and integrity of

8. "Application A" is designed for mobile chatting or messaging. To use this application, a user downloads the application to a mobile phone or other mobile device via a service such as Google Play Store, Apple iTunes, or another similar provider. Once downloaded and installed, the user is prompted to create an account and username. The user also has a display name, which is what other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature, and the two parties can then send each other messages, images, and videos.

9. "Application A" users are also able to create chat groups, of up to 50 people, to communicate in a group setting and exchange images and videos. These groups are administered by the group creator who has the authority to remove and ban other users from the created group. Once the group is created, "Application A" users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a "hashtag" that is easily identifiable or searchable by keyword. (A "hashtag" refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic).

10. SPS was able to log in and secure John Doe's "Application A" account. In reviewing the chat conversations held with John Doe's account, SPS was able to identify 78 unique "Application A" users who had shared at least one image or video of child

---

the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the application will be identified herein as "Application A."

pornography with John Doe directly, or who had posted child pornography in one of the "Application A" groups to which John Doe belonged, and six "Application A" users who had posted a message between or commented on child pornography images or videos. Many of the groups to which John Doe belonged had names that included terms that your affiant knows through training and experience to be suggestive of child pornography.

11. SPS logged all of the information regarding the messages and saved all of the images and videos of child pornography shared with John Doe's account. SPS sent preservation requests to "Application A" regarding all 78 accounts referenced in the previous paragraph between April 20 and April 30, 2016. SPS transmitted to HSI the information logged and saved from the review of John Doe's "Application A" account.

12. On June 28, 2016, a Production Order was issued by a Provincial Court Judge in Saskatchewan, Canada, ordering "Application A" to produce user information and saved content regarding these 78 accounts. On September 15, 2016, SPS received the requested results from "Application A." The information received from "Application A," including the Certification of Records provided by "Application A," was transmitted to HSI, along with a copy of the Production Order issued by the Provincial Court Judge.

13. The results provided by "Application A" included, among other things, additional images and videos of child pornography recently shared by the 78 accounts. This included both child pornography shared with John Doe and child pornography shared with other individuals and groups not related to John Doe's account. Additional Production Orders were served on "Application A" for information regarding the "Application A"

accounts who shared child pornography with the originally investigated 78 accounts, leading to the identification of additional "Application A" accounts beyond the 78 accounts that shared child pornography with John Doe.

14. Your affiant has reviewed the information received from "Application A." A review of that information shows that between February 23, 2016 and March 11, 2016 an "Application A" user with the account name "mrningstr" used "Application A" to share images and videos of child pornography. Specifically, the images and videos shared by "mrningstr" included the following:

a. "**1456199300987-4d512a61-1d79-4707-a796-eeb0d794ad75**" – a video file depicting what appears to be a 4-5 year old prepubescent female child watching an adult male stroke his penis and attempting to get the female child to touch his penis as well.

b. "**1456201966742-e087d7333-6a51-4797-8052-933f503dbe32**" – a video file depicting what appears to be a naked 4-5 year old prepubescent female child lying on her back while an adult male holds her head and ejaculates in her mouth.

c. "**1456409923486-65cde1f8-bcde-4be6-a9c9-4510414ef66c**" – a video file depicting what appears to be a 3-4 year old prepubescent female child on her hands and knees, naked from the waist down. An adult male penetrates the child with his penis from behind.

I have viewed each of the above video files and, based on my training and experience, can confirm that each constitutes child pornography as defined in 18 U.S.C. § 2256(8).

15. On or about October 14, 2016, a federal administrative summons was issued to "Application A" for subscriber and IP information associated with the "Application A" user "mrningstr." The information provided by "Application A" included the following:

Subscriber First Name:	Ja
Subscriber Last Name:	Ca
Subscriber Email Address:	shdwdom@gmail.com
Last IP Address login:	67.253.234.152 on July 16, 2016

16. On or about February 13, 2017, another federal administrative summons was issued to "Application A" to confirm the subscriber information associated with the "Application A" user "mrningstr." The information provided by "Application A" included the following:

Subscriber First Name:	Ja
Subscriber Last Name:	Ca
Subscriber Email Address:	shdwdom@gmail.com
Last IP Address login:	67.253.234.152 on December 18, 2016

17. A query of the American Registry for Internet Numbers ("ARIN") online database revealed that IP address 67.253.234.152 is registered to Charter Communications (formerly Time Warner Cable). On June 20, 2017, a summons was issued to Time Warner Cable in regard to IP address 67.253.234.152. According to Time Warner Cable, Janette DANIEL, 2001 New Street, Ontario, NY 14519 was the subscriber for IP address 67.253.234.152 and had been since June 2016.

18. A check of publicly available databases revealed that David W. DANIEL Sr. and the SUBJECT (David W. DANIEL Jr.) have resided at 2001 New Street, Ontario, NY with Janette Daniel in the past. Public records also indicate that Janette DANIEL has been deceased since January 2016.

19. According to records from the New York State Department of Motor Vehicles, the SUBJECT (David W. DANIEL, Jr.), has a current listed address at the

SUBJECT PREMISES (102 Mitchell Lane, Hamlin, New York, 14464), and a prior listed address of 2001 New Street, Ontario, NY 14519, where IP address 67.253.234.152 was registered.

20. On August 14, 2017, a summons was issued to "Application A" for the username "mrningstr" requesting updated subscriber and IP address information. On August 16, 2017, "Application A" provided information that the subscriber name used for "mrningstr" remained "Ja Ca" with the same associated email address of "shdwdom@gmail.com." This has remained consistent since the account was discovered by law enforcement in 2016. The response also included the last IP address used by "mrningstr." Specifically, on July 30, 2017, IP address 67.240.201.61 was used by "mrningstr" to access "Application A." A query of the American Registry for Internet Numbers ("ARIN") online database revealed that IP address 67.240.201.61 is registered to Charter Communications (formerly Time Warner Cable).

21. On August 17, 2017, a summons was issued to Charter Communications requesting subscriber information for IP address 67.240.201.61 for the date July 30, 2017. On August 21, 2017, Charter Communications responded to the summons by providing the following subscriber information for IP address 67.240.201.61 for the date July 30, 2017:

NAME:	David Daniel
ADDRESS:	161 Victor Lane Apt. 102
	Hamlin, New York 14464
PHONE:	585-766-XXXX

22. The address provided by Charter Communications, 161 Victor Lane, is the street address for the Bradford Manor Apartments, Hamlin, NY. The SUBJECT PREMISES is a specific apartment, number 102, within the Bradford Manor Apartments. Mitchell Lane intersects with Victor Lane within the Bradford Manor Apartment complex, and the SUBJECT PREMISES, apartment 102, is physically located on Mitchell Lane at the intersection with Victor Lane.

23. To clarify the discrepancy between the Charter response and the SUBJECT PERSON'S known address of 102 Mitchell Lane, HSI interviewed the apartment manager at Bradford Manor. When asked about the location of "161 Victor Lane, Apt. 102," the apartment manager directed HSI to the SUBJECT PREMISES (102 Mitchell Lane). There, HSI observed a mailbox with the words "Daniel/Beach" and "102 Mitchell" written on it (see Attachment "A"). Accordingly, it appears that when subscribing for Charter internet service, the occupant of 102 Mitchell Lane inadvertently indicated "Victor Lane" rather than "Mitchell Lane" in order to designate apartment 102 within the Bradford Manor Apartments, which is located at the intersection of Mitchell and Victor Lanes. On November 13, 2017, the Bradford Manor management office again confirmed that the correct address for apartment 102 (the SUBJECT PREMISES) is 102 Mitchell Lane and not "161 Victor Lane, Apt. 102." The management office further confirmed that the SUBJECT PREMISES is the only apartment designated as 102 within the entire Bradford Manor complex and that the SUBJECT PERSON resides at the SUBJECT PREMISES.

24. On October 18, 2017, I conducted public and law enforcement database research, which confirmed that the SUBJECT currently resides at the SUBJECT

PREMISES, 102 Mitchell Lane, Hamlin, New York. In addition, these databases indicate that the SUBJECT had previously resided at 2001 New Street in Ontario, New York from on or about 1990 through the beginning of 2017.

PAST CHILD EXPLOITATION CONDUCT/ACTIVITY OF DAVID W DANIEL

25. On July 20, 2006, SUBJECT PERSON, David W. DANIEL, Jr., pleaded guilty to a violation of New York State Penal Law 263.11, Possessing an Obscene Sexual Performance By a Child Less Than 16 years old. DANIEL was sentenced to 30 days incarceration, followed by ten years of sex offender probation. DANIEL completed his probation term in July 2016.

26. Paragraphs 6-25 above establish cause to believe that David W. DANIEL Jr. is user of the "Application A" username "mrningstr" and that he has moved from the address of 2001 New Street, Ontario, New York to 102 Mitchell Street, Hamlin, New York.

CHARACTERISTICS OF CHILD EXPLOITATION VIOLATORS

27. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the possession, receipt and distribution of child pornography:

a. Those who receive and attempt to receive child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in

sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who receive and attempt to receive child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who receive and attempt to receive child pornography often possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, those who receive and attempt to receive child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and

surrounding area. These collections are often maintained for several years and are kept close by, usually at the individual's residence, to enable the collector to view the collection, which is valued highly.

e. Those who receive and attempt to receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Those who receive and attempt to receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if the SUBJECT PERSON uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in the SUBJECT PREMISES or on the SUBJECT PERSON as set forth in Attachment A.

28. Based upon general life experience and my training and experience in criminal investigations, I know that people who move from one residence to another almost always bring their personal belongings with them, to include, computers, internal/external

electronic storage devices, mobile electronics and other items listed in Attachment B, as these items often contain personal information and items like personal mementos, such as family pictures, videos, word processing and spreadsheet documents, applications, software, and other data that will continue to be used by the owners of such equipment after moving to their new residence. Finally, as mentioned in paragraph 27 above, individuals involved in the possession, distribution, and production of child pornography typically treat their child pornography as a collection that is highly valued, maintained for several years, and stored close-by, usually in a private space maintained by the individual where it can be accessed easily. Accordingly, there is probable cause to believe that evidence of the possession, receipt and distribution of child pornography was transferred from DANIEL'S former residence to his new residence at the SUBJECT PREMISES, and may be found there or on the SUBJECT PERSON.

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, CELLULAR TELEPHONES AND THE INTERNET

29. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one

of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone or external media in most cases.

g. A cellular telephone is a handheld wireless device used for voice and data communication through radio signals. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on

personal calendars; and accessing and downloading information from the Internet. The capability of a cellular telephone to store images in digital form makes the cellular telephone itself an ideal repository for child pornography.

h. Individuals can use online resources to retrieve, store and share child pornography, including services offered by Internet Portals such as Google, America Online (AOL), Yahoo! and Hotmail, among others. Online services allow a user to set up an account providing e-mail and instant messaging services, as well as electronic storage of cellular telephone files in any variety of formats. A user can set up an online storage account from any cellular telephone with access to the Internet. Evidence of such online storage of child pornography is often found on the user's cellular telephone. And even in cases where online storage is used, evidence of child pornography can be found on the user's cellular telephone in most cases.

i. The interaction between software applications and the cellular telephone operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a cellular telephone hard drive without the user's knowledge. As a result, digital data that may have evidentiary value to this investigation could exist in the user's cellular telephone media despite, and long after, attempts at deleting it.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES or on the SUBJECT

PERSON, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive, on the defendant's cellular phone, or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. I submit that if a computer or storage medium is found in the SUBJECT PREMISES or on the SUBJECT PERSON, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. .

b. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

32. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe

that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES or on the SUBJECT PERSON because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user

account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

33. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. It is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to

conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which

means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

34. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that

individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

35. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

REQUEST FOR SEALING OF WEBSITE/AFFIDAVIT

36. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this Application, including the Application, Affidavit, and Search Warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the SUBJECT PREMISES and with the SUBJECT PERSON). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through forums. Premature disclosure of the contents of this Affidavit and related documents may have a significant and negative

impact on this continuing investigation and may jeopardize its effectiveness by alerting potential targets to the existence and nature of the investigation, thereby giving them an opportunity to flee, or to destroy or tamper with evidence.

CONCLUSION

37. Based on my training and experience, I know that users of websites/applications such as "Application A" can and do use these websites/applications via a smartphone, tablet, or other mobile device. Further, based on my training and experience, I know that individuals often keep their smartphones, tablets, or other mobile devices on their person (for example, in a pocket, in a bag, or in a hand), especially when they are outside of their homes.

38. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located at the SUBJECT PREMISES or on the SUBJECT PERSON, wherever he may be. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES and SUBJECT PERSON described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

39. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless

otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

JUSTIN BURNHAM
SPECIAL AGENT
HOMELAND SECURITY INVESTIGATIONS

Sworn and subscribed before me
this 16 day of November, 2017.

JONATHAN W. FELDMAN
UNITED STATES MAGISTRATE JUDGE